

REMARKS

Claims 1-20 are pending in the application, where Claims 1, 8, 15 and 18 are the independent claims. Claims 1, 3-4 and 6-22 will be pending after entry of this amendment. Base Claims 1 and 15 are being amended. Support for these claim amendments can be found at least on page 6, line 14 through page 7, line 8 of Applicant's Specification, as originally filed. New Claims 21 and 22 are being added. Support for these new claims can be found at least on page 7, lines 17-28 of the Specification, as originally filed. Claims 2 and 5 are being canceled. No new matter is being introduced by way of these amendments.

Regarding New Claims

New Claims 21 and 22 are being added. Support for these new claims can be found at least on page 7, lines 17-28 of the Specification, as originally filed. No new matter has been introduced by way of these claim additions.

New Claim 21 includes limitations ("...i) using a first key pair from the set of at least one key pair to encrypt a first electronic message, the first key pair associated with a valid first validity field; and ii) in an event the first validity field is not valid with respect to a second electronic message, using a second key pair from the set of at least one key pair to encrypt the second electronic message, the second key pair associated with a valid second validity field") which are not shown or described in the Schneier reference or the Examiner's Official Notice. Accordingly, the Applicant respectfully submits new Claim 21 should be allowed.

New Claim 22 recites similar limitations as new Claim 21, and as such is allowable for at least the same reasons. Accordingly, the Applicant respectfully submits new Claim 22 should be allowed.

Regarding Canceled Claims

Claims 2 and 5 are being canceled without prejudice or disclaimer.

Regarding Allowed Claims

The Applicant acknowledges and kindly thanks the Examiner for allowing Claims 8-14.

§ 102(b) Rejection

Claims 1, 15 and 18 have been rejected under 35 U.S.C. 102(b) as being anticipated by Schneier et al. (U.S. Patent No. 5,978,475, hereinafter, "Schneier").

Amended base Claim 1 recites, in part, "creating an index value that is uniquely associated with the key pair and both the sender and the receiver, the index value utilized for key retrieval," and "storing in a key server at least the encrypted private key together with the associated index value," where the underlined text are limitations added by way of amendment in the Claim Listing above.

Describing the Applicant's claimed invention briefly, the claimed invention generates a new ad hoc asymmetric key pair uniquely associated with both sender and receiver. An index value that is uniquely associated with the key pair is also generated. Consequently, the index value is uniquely associated with: i) the key pair and ii) both the sender and the receiver. Furthermore, the Applicant's claimed invention uses the index value for key retrieval.

By creating an index value that is uniquely associated with the key pair and both the sender and the receiver, and utilizing the index value for key retrieval, the claimed invention allows a sender to generate, without the receiver's involvement, an ad-hoc public-private key pair whose private key is known only to the sender. Moreover, by doing so, the claimed invention generates the ad-hoc public-private key pair to allow the sender to encrypt a message even in the case that: i) there is no known receiver public key for the sender to use, ii) the receiver is not online to participate in a key negotiation protocol to set up a shared key with the sender, iii) an out-of-band shared key distribution between the sender and the receiver is not practical, or iv) it is more secure for the sender to be able to use a public key instead of accessing a stored secret shared key to encrypt the sender's multiple messages.

In contrast, the Schneier reference does not teach nor does it suggest an index value which is uniquely associated with a key pair, and both a sender and a receiver, and which is used to retrieve the key pair. Firstly, Schneier describes deriving an encryption/decryption key using an algorithm. Schneier's encryption key is derived, using a "one-way process," described in column 11, lines 24-60 and illustrated in FIG. 5. *See also* column 13, lines 5-10. Schneier's deriving an encryption/decryption key is not the same as the Applicant's using an index value to retrieve a key.

Secondly, Schneier describes destroying encryption keys immediately after use and then regenerating an encryption key before a user can be given a key (so that user can decrypt and read). Schneier, column 11, line 64 - column 12, line 1, and column 12, lines 31-37. The Applicant respectfully submits that it does not make sense for Schneier to use an index value to retrieve a key which is readily derived and immediately destroyed. With such a key, an index value serves no purpose or utility. As such, the Schneier reference neither teaches nor provides motivation for using an index value for key retrieval.

In addition to failing to teach or provide motivation for using an index value to retrieve a key, the Schneier reference fails to describe storing a key in a key server, as claimed by Claim 1. Again, because Schneier immediately destroys an encryption key after use and then regenerates an encryption key in order to give a user a key to decrypt and read, the Applicant respectfully submits that it does not make sense for Schneier to store such a key. Even if Schneier did store an encryption/decryption key (which it does not) the Schneier reference is silent as to storing the encryption/decryption key in a key server.

In fact, Schneier discloses but only within the limited context of asymmetric or “public-key” cryptography, storing a decryption key, “somewhere off-line,” to prevent ready access, such as by an attacker. Schneier, column 15, lines 1-24. Schneier’s storing somewhere off-line is not the same as the Applicant’s storing in a key server. As such, the Schneier reference neither teaches nor provides motivation for storing a key, let alone storing in a key server, as recited in base Claim 1 (“storing in a key server at least the encrypted private key together with the associated index value”).

Lastly, the Schneier reference describes enhancing the disclosed technique with additional security features afforded by public-key cryptography. Schneier, column 14 line 55 – column 15 line 24. Schneier provides multiple examples of such enhancements (e.g., encrypting data with the public key of the intended recipient). Schneier’s examples, however, all fall short of teaching or providing motivation for the Applicant’s base Claim 1 (“encrypting the private key, the private key known only to the sender”).

Independent Claims 1 and 15 have similar limitations and should also be allowable for at least the same reasons presented above. As such, the rejection under 35 U.S.C. § 102(b) of Claims 1 and 15 is believed to be overcome. Allowance of these claims is respectfully requested.

Independent Claim 18 recites similar limitations as allowed Claim 8. As such, the Applicant respectfully submits, Claim 18 is allowable for at least the same reasons as Claim 8. Withdrawal of the § 102 rejection of Claim 18 and allowance of this claims are thus respectfully requested.

§ 103(a) Rejection

Claims 2, 3, and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in further view of the Examiner taking Official Notice.

The Official Notice, similar to the Schneier reference, does not teach or suggest the Applicant's using an index value and storing an encrypted private key together with the associated index value in a key server. Therefore, the Official Notice, does not add to Schneier the missing claim elements of, "creating an index value that is uniquely associated with the key pair and both the sender and the receiver, the index value utilized for key retrieval," and "storing in a key server at least the encrypted private key together with the associated index value," as claimed in base Claim 1.

Thus, no combination of Schneier and the Official Notice imply, suggest or provide motivation for the method as claimed in base Claim 1. Claim 3 depends from base Claim 1 and thus inherits this claim limitation. Claims 2 and 5 are canceled without prejudice or disclaimer. Thus, the § 103 rejection of Claims 2, 3 and 15 as being unpatentable over Schneier in view of the Official Notice is believed to be overcome. Allowance of Claim 3 is respectfully requested.

Objected Claims

Claims 4, 6, 7, 16, 17, 19, and 20 have been objected to as being dependent upon rejected base claims. Dependent Claims 4, 6 and 7 depend from base Claim 1. Dependent Claims 16 and 17 depend from base Claim 15. Dependent Claims 19 and 20 depend from base Claim 18.

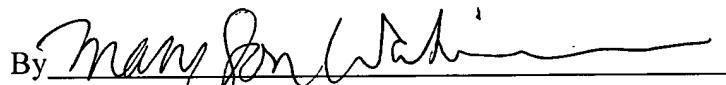
Thus, the foregoing arguments regarding base Claims 1, 15 and 18 also apply to each of the dependent claims. Allowance of these claims is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims, which will be pending after entry of this Amendment, Claims 1, 3, 4, and 6-22 are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By 
Mary Lou Wakimura
Registration No. 31,804
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133

Dated: 11/27/06